REMARKS

The Examiner has rejected Claims 7-27 under 35 U.S.C. 101 as being directed toward non-statutory subject matter. Applicant has clarified independent Claims 7 and 17 to include a computer program product "embodied on a tangible computer readable medium" in order to avoid such rejection.

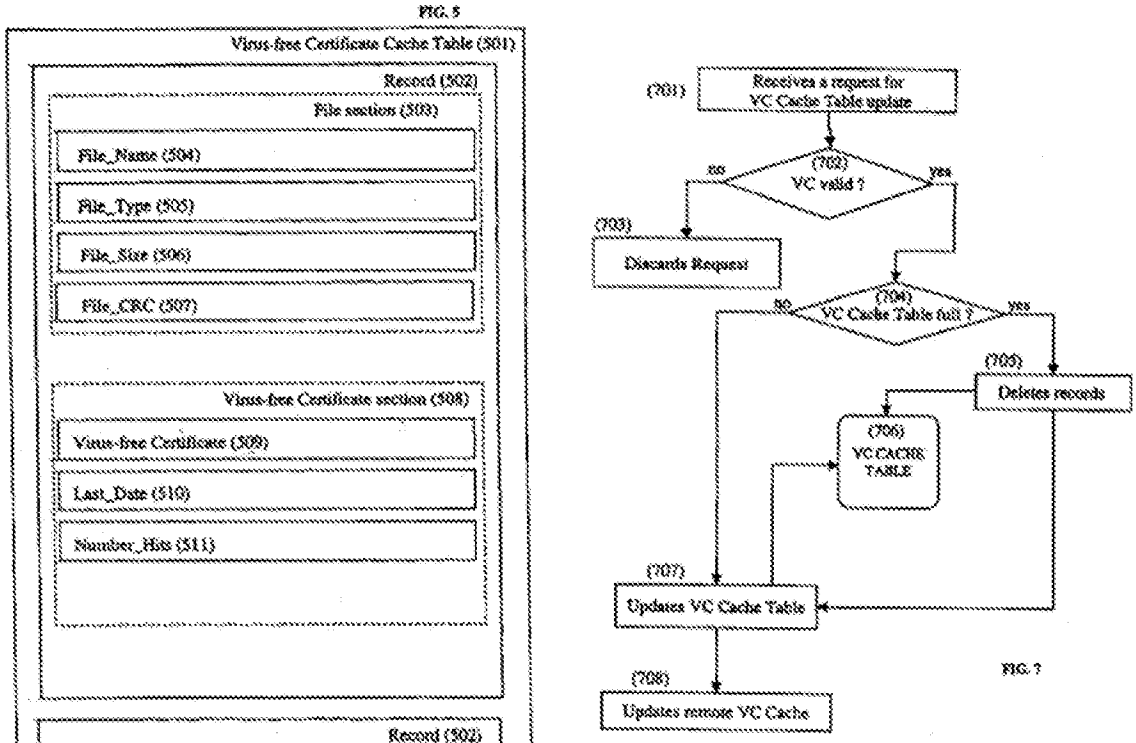
The Examiner has rejected Claims 7-13, 16-24, 27, 34-40, 43-51, 54, 61-67, 70-78, and 81 under 35 U.S.C. 103(a) as being unpatentable over Hruska et al. (U.S. Patent No. 6,195,587), in view of Le Pennec et al. (U.S. Patent No. 6,892,303). Further, the Examiner has rejected Claims 14-15, 25-26, 41-42, 52-53, 68-69, and 79-80 under 35 U.S.C. 103(a) as being unpatentable over Hruska, in view of Le Pennec, further in view of Caccavale (U.S. Patent Publication No. 2002/0129277). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of dependent Claim 14 et al.

With respect to the independent claims, the Examiner has relied on the following excerpts from Hruska and Le Pennec to make a prior art showing of applicant's claimed technique "wherein said assessment computer stores a database of computer files and said database includes for each computer file a persistence flag indicating whether an entry relating to said computer file should be purged from said database during purge operations" (see this or similar, but not necessarily identical language in the independent claims).

> "If the file is then authorized by the supervisor, its checksum as calculated by the file server is added to the file server's list of checksums of authorized files (box 27) and a report message is returned to the relevant workstation indicating that access to the file can be allowed (box 22)." (Hruska, Col. 5, lines 14-18 - emphasis added)

> "This procedure may be used in addition to the inclusion in files of data indicating whether the file has been authorized or barred from use (not illustrated in FIGS. 3a or 3b)." (Hruska, Col. 5, lines 22-25 - emphasis added)

"It is an object of the present invention to improve current anti-virus checking methods and to provide a new method using file Certificates similar to X.509 Certificates used to authenticate an identity. A specific process associates a Certificate, called virus-free Certificate (VC), with a file in order to speed up and improve the virus detection." (Le Pennec, Col. 5, lines 29-34 - emphasis added)



(Le Pennec, Fig. 5, and Fig. 7)

Applicant respectfully asserts that the excerpts from Hruska relied upon by the Examiner merely teach that "[a file's] checksum…is added to the file server's list of checksums of authorized files" and that "[t]his procedure may be used in addition to the inclusion in files of data indicating whether the file has been authorized or barred from use." However, Hruska's disclosure of an authorized file's checksum being stored in a file server's list of checksums in no way suggests a technique "wherein said assessment computer stores a database of computer files" (emphasis added), as claimed by applicant. Clearly a list of checksums, where such checksums are of the files, as in Hruska, does not meet applicant's claimed database of computer files, as claimed.

In the Office Action dated 03/27/2007, the Examiner has argued that 'the combination of Hruska and Le Pennec replaces the checksum database with the database of virus-free certificates which falls within the scope of "computer file".'

Applicant respectfully disagrees. Le Pennec simply teaches that "[a] specific process associates a Certificate, called virus-free Certificate (VC), with a file" (emphasis added). However, merely teaching the association of a certificate with a file, does not teach a technique "wherein said assessment computer stores a database of computer files" (emphasis added), in the context claimed by applicant.

In particular, applicant notes that Le Pennec discloses that "the only process performed by the system receiving the file…is to verify the file against the file signature included in the virus-free Certificate" (Col. 6, lines 3-6). Clearly, a database of certificates that is used to verify the file, as in Le Pennec, cannot meet applicant's claimed "database of computer files," particularly since such "database includes for each computer file fields specifying…data identifying said **requesting computer**," where the "computer file [is] to be accessed by said requesting computer" (see the same or similar, but not necessarily identical language in the independent claims - emphasis added), in the context claimed.

Furthermore, applicant respectfully asserts that the figures and associated excerpt from Le Pennec relied upon by the Examiner simply teach "[a] specific process [that] associates a Certificate, called virus-free Certificate (VC), with a file in order to speed up and improve the virus detection." Additionally, Le Pennec discloses a "Virus-free Certificate Cache Table, [which] is dynamically built by the VCC and comprises a local copy of Virus-free Certificate which have been transmitted through the LAN/WAN network" and that "[t]he table (501) comprises for each file, one or multiple associated Virus-free Certificates" (Col. 14, line 66-Col. 15, line 4 – emphasis added).

In addition, Le Pennec discloses that the Virus-free Certificate Section includes fields for a "Virus-free Certificate (509)," a "Last_Date (510)," and a "Number_Hits

(511)" (Fig. 5), where the "(511) Number_Hits ... is the number of requests (hits) that have been received by the VC Cache to retrieve this VC" and that "[t]ypically, this number of hits is used when the VC Cache is maintained and when for instance the records with the lowest number of hits have to be deleted" (Col. 15, lines 50-54 – emphasis added). Further, Le Pennec discloses that '(704) tests whether or not the VC Cache Table is full: If the VC Cache Table is full: (705) deletes some record of the VC Cache Table (706)" and "[t]ypically, the records which are deleted are selected according to the "Last_Date" and "Number_Hits" fields' (Col. 17, lines 58-64 – emphasis added).

However, the mere disclosure that the Number_Hits are used when the VC Cache Table is full and the records with the lowest number of hits have to be deleted, as in Le Pennec, in no way suggest a technique "wherein said assessment computer stores a database of computer files and said database includes for each computer file a persistence **flag** indicating whether an entry relating to said computer file should be purged from said database during purge operations" (emphasis added), as claimed by applicant. Clearly, allowing a record to be deleted when the table is full based on the Last_Date and Number_Hits fields, especially where such Number_Hits field identifies a number of hits, fails to suggest any sort of "persistence flag," in the manner as claimed by applicant.

In the Office Action dated 03/27/2007, the Examiner has argued that '[t]he claim requires that the "persistence flag" indicate[s] whether an entry in the database should be purged from said database during purge operations' and that '[t]he "number of hits" is used to determine which entries will be removed from the database during purging (when the database is full and a new entry is to be added).'

Applicant respectfully disagrees and points out that Le Pennec simply discloses that the "Number_Hits ... is the number of requests (hits) that have been received by the VC Cache to retrieve [a Virus-free Certificate]" and that "this number of hits is used when the VC Cache is maintained and when for instance the records with the lowest number of hits have to be deleted" (emphasis added). However, merely storing the **number** of requests to retrieve a certificate in a record, in addition to maintaining a cache

and deleting records with the lowest number of hits, as in Le Pennec, does not specifically disclose any sort of a persistence **flag**, as claimed, let alone "a persistence flag indicating whether an entry relating to said computer file should be purged from said database during purge operations" (emphasis added), as claimed by applicant.

Additionally, with respect to the independent claims, the Examiner has relied on Figure 5, element 504 (reproduced above) and Figure 3, element 304 from Le Pennec, to make a prior art showing of applicant's claimed technique "wherein said database includes for each computer file fields specifying a filename of said computer file, data identifying said requesting computer and a storage location of said computer file."

Applicant respectfully asserts that, in Le Pennec, "FIG. 5 describes the Virus-free Certificate Cache Table according to the present invention" (see Col. 6, lines 46-47), and that "[i]n the VC Cache Table..., each file is identified by...the file name, the file type, optionally, the file size, [and] the file CRC" (see Col. 15, lines 5-10 – emphasis added). However, merely disclosing that the file is identified by the file name, file type, file size, and file CRC, as in Le Pennec, fails to even suggest a technique "wherein said database includes for each computer file fields specifying a filename of said computer file, data identifying said requesting computer and a storage location of said computer file, and a checksum value calculated from said computer file" (emphasis added), as claimed by applicant.

Further, in the Office Action dated 03/27/2007, the Examiner has argued that 'Le Pennec does in fact teach the database having fields for "a filename of said computer file" as seen in Fig. 3 Element 305, "data identifying said requesting computer and a storage location of said computer file" as seen in Fig. 3 Element 304 and Col. 10 Lines 27-32, and "a checksum value calculated from said computer file" as seen in Fig. 5 Element 507.'

Applicant respectfully disagrees and asserts that item 304 in Figure 3 of Le Pennec simply discloses an identifier for a source system, such as "the IP address of the

File Server which has originated all files within a specific software company" (Col. 10, lines 26-31). Clearly, Le Pennec's disclosure of an identifier of a source of a file, as relied on by the Examiner, fails to disclose that "said database includes for each computer file fields specifying...data identifying said requesting computer," particularly where "a computer file [is] to be accessed by said requesting computer" (emphasis added), in the context claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of dependent Claim 14 et al. into the independent claims.

With respect to the subject matter of Claim 14 et al. (now at least substantially incorporated into the independent claims), the Examiner has relied on Col. 4, lines 55-57 from the Hruska reference, in addition to paragraph [0075] of the Caccavale reference, to make a prior art showing of applicant's claimed technique "wherein said assessment computer is operable in at least a higher level security mode and a lower level security mode, said assessment computer serving to deny access to a greater range of computer files when operating in said higher level security mode compared with said lower level

security mode" (see this or similar, but not necessarily identical language in the independent claims). Applicant respectfully notes that the Examiner has cited "Hruska Paragraph 0075" on Page 8 of the Office Action dated 03/27/2007, which applicant interprets as paragraph [0075] of the Caccavale reference.

Applicant respectfully points out that the above excerpt from Hruska relied on by the Examiner merely teaches that "an operator of the workstation can instruct the validity of any or all files stored for access by the workstation to be checked" (Col. 4, lines 55-57 – emphasis added). Further, applicant notes that the above excerpt from Caccavale simply teaches that when a "virus checker program is incapable of detecting a new virus… the supplier of the anti-virus program will distribute an updated pattern file that may be used by the conventional virus checker program to detect the new virus" (paragraph [0075] – emphasis added).

However, only teaching that an operator can instruct file validity to be checked, as in Hruska, and that an anti-virus program supplier distributes an updated pattern file to detect a new virus, as in Caccavale, does not even suggest a technique "wherein said assessment computer is operable in at least a higher level security mode and a lower level security mode, said assessment computer serving to deny access to a **greater range** of computer files when operating in said higher level security mode compared with said lower level security mode" (emphasis added), as claimed by applicant. Clearly, the operator instructing for the validity of all files stored for access to be checked, as in Hruska, simply fails to even suggest that "said assessment computer serv[es] to deny access to a **greater range** of computer files when operating in said higher level security mode compared with said lower level security mode" (emphasis added), in the manner as claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 12 et al., the Examiner has relied on Col. 5, lines 14-18 from the Hruska reference to make a prior art showing of applicant's claimed technique "wherein said database of computer files specifies whether respective computer files contain malware" (see this or similar, but not necessarily identical language in the aforementioned claims).

Applicant respectfully points out that the above excerpt from Hruska relied on by the Examiner merely teaches that "[i]f the file is then authorized by the supervisor, its checksum... is added to the file server's list of checksums of authorized files" and that "a report message is returned to the relevant workstation indicating that access to the file can be allowed" (Col. 5, lines 15-19 – emphasis added). Thus, the list of checksums disclosed in Hruska only includes checksums for which files are authorized, which does not teach or suggest that "said database of computer files specifies whether respective computer files contain malware" (emphasis added), as claimed. In fact, applicant respectfully points out that since the checksums in Hruska are only added to the list of checksums if the associated files are authorized, such list of checksums is only associated with authorized files, such that there would be no need to "[specify] whether respective computer files contain malware," as applicant claims.

Additionally, applicant notes that Hruska teaches "the inclusion in files of data indicating whether the file has been authorized or barred from use" (Col. 5, lines 23-25 – emphasis added). However, merely including in a file data indicating whether the file is authorized or barred, as in Hruska, does not teach a technique "wherein said database of computer files specifies whether respective computer files contain malware" (emphasis added), as claimed by applicant.

Additionally, with respect to Claim 15 et al., the Examiner has relied on Col. 4, lines 55-57 from the Hruska reference, in addition to paragraph [0075] of the Caccavale reference, to make a prior art showing of applicant's claimed technique "wherein said

assessment computer is triggered to change from said lower level security mode to said higher level security mode by a lock down trigger message received at said assessment computer from a remote computer" (see this or similar, but not necessarily identical language in the independent claims). Applicant respectfully notes that the Examiner has cited "Hruska Paragraph 0075" on Page 8 of the Office Action dated 03/27/2007, which applicant interprets as paragraph [0075] of the Caccavale reference.

Applicant respectfully asserts that the above excerpt from Hruska relied on by the Examiner merely teaches that "an operator of the workstation can instruct the validity of any or all files stored for access by the workstation to be checked" (Col. 4, lines 55-57 – emphasis added). Additionally, applicant points out that on Page 8 of the Office Action dated 03/27/2007 the Examiner admits that "Hruska… fail[s] to disclose a message being sent to the file server indicating a switch to a mode of operation wherein more files are denied for access." Further, applicant respectfully asserts that the excerpt from Caccavale simply teaches that when a "virus checker program is incapable of detecting a new virus… the supplier of the anti-virus program will distribute an updated pattern file that may be used by the conventional virus checker program to detect the new virus" (paragraph [0075] – emphasis added).

However, teaching that an operator can instruct file validity to be checked, in addition to teaching that an anti-virus program supplier distributes an updated pattern file to detect a new virus, does not even suggest a technique "wherein said assessment computer is triggered to change from said lower level security mode to said higher level security mode by a lock down trigger message received at said assessment computer from a remote computer" (emphasis added), as claimed by applicant.

Again, since at least the third element of the *prima facie* case of obviousness has not been met, as noted above, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 83-84 below, which are added for full consideration:

> "wherein said file access clearance response indicates access to said computer file is denied if said computer file has previously been identified as containing malware, and said denied access response includes deletion of said computer file" (see Claim 83); and
>
> "wherein said higher level security mode includes banning access to at least one predetermined format of computer files" (see Claim 84).

Again, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P468).

Respectfully submitted,
Zilka-Kotab, PC.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100